

Abstract

A conditional access system for multimedia data is disclosed that offers acceptable security at drastically reduced requirements on hardware performance. A selectively encrypted transport stream is formed from a clear transport stream
5 by detecting particular data packets within the clear transport stream, removing and encrypting the particular data packets with an event encryption key, and inserting the encrypted data packets into the remaining clear transport stream at insertion positions corresponding to the original positions of the particular data packets in the clear transport stream. For specific embodiments that include
10 decryption circuitry inside a user smart card, the level of security of such system is even higher than that of conventional ones.

BEST AVAILABLE COPY